iFace: A Deepfake Resilient Digital Identification Framework for Smart Cities

Presenter: Alakananda Mitra

A. Mitra[1], S. P. Mohanty[2], P. Corcoran[3], and E. Kougianos[4]

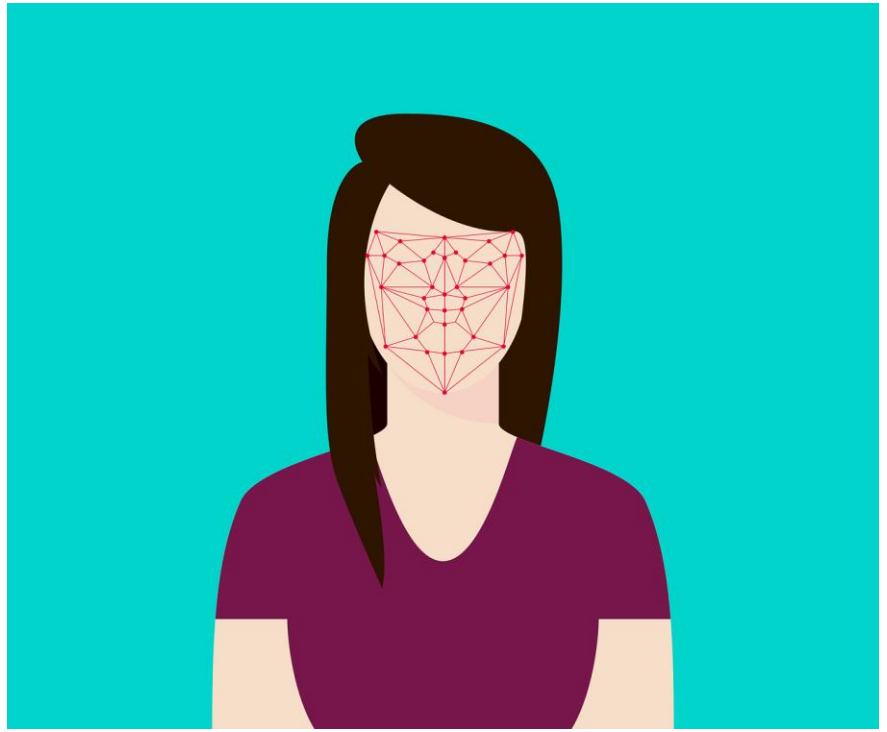
University of North Texas, Denton, TX , USA.[1,2,4] and

National University of Ireland, Galway, Ireland[3].

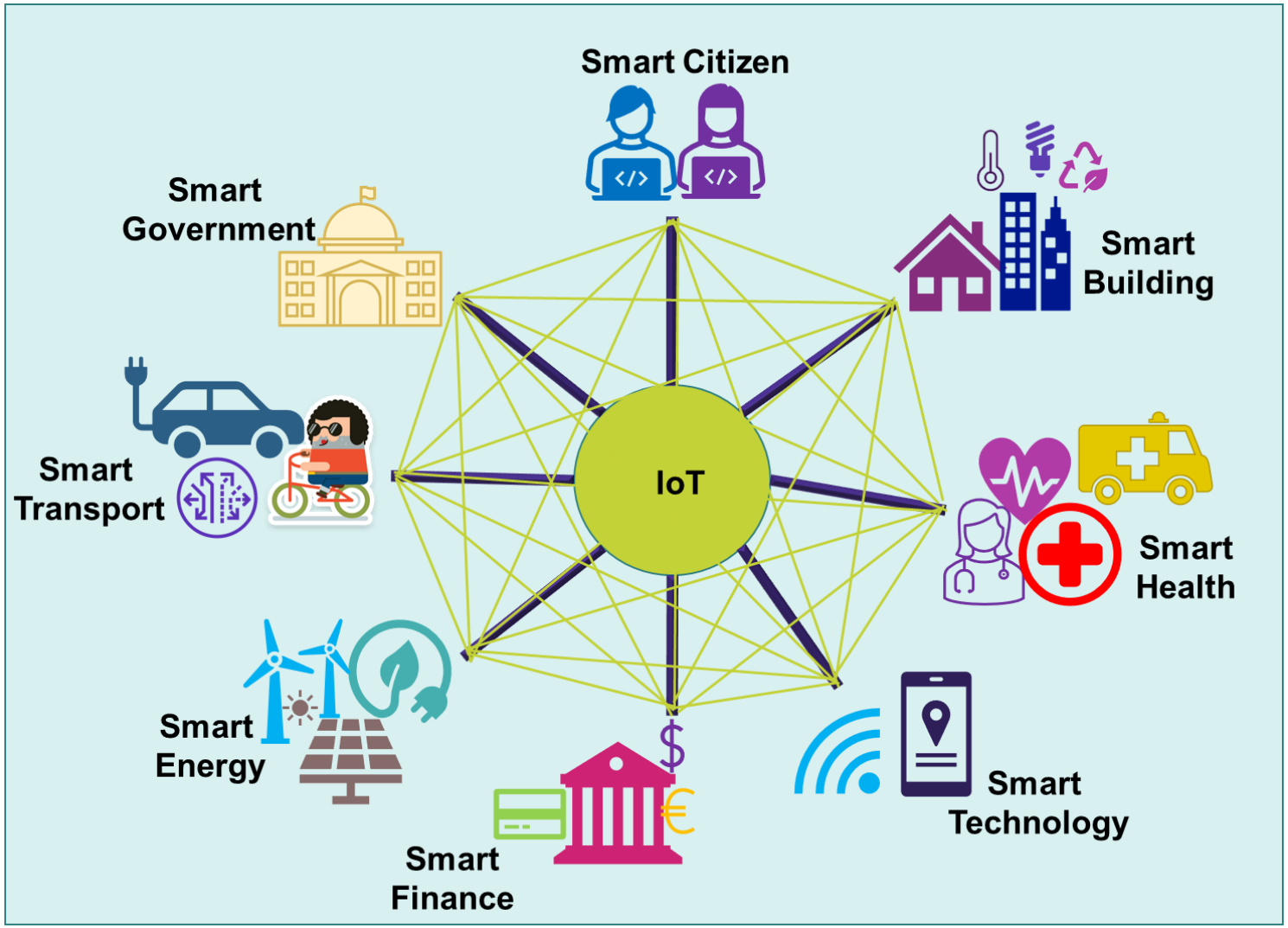
Email: **alakanandamitra@my.unt.edu[1], saraju.mohanty@unt.edu[2], peter.corcoran@nuigalway.ie[3], and elias.kougianos@unt.edu[4]**

Outline

- Smart City & Digital ID
- iFace: Digital ID System
- iFace Resilient to Various Attacks
- iFace Implementation
- iFace Performance Evaluation
- Conclusions & Future Work

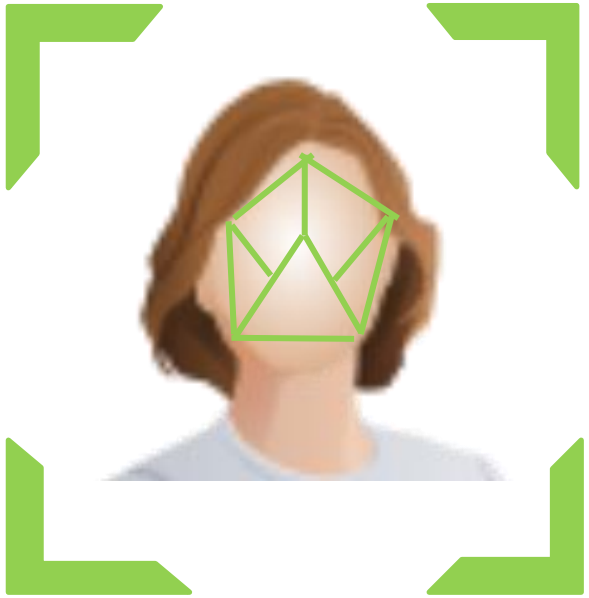


Smart City Components



Digital Identification (ID)

- Person Specific
- Unique
- Bio-metrics Based
- No Need to Keep Any Secret Key
- User Him/Herself is His/Her Secret Key
- Gateway of Smart City
  - Robust
  - Resilient to Attacks



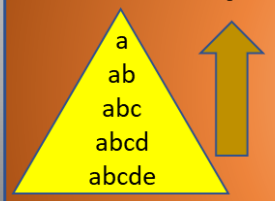
Challenges of Digital ID

Biometrics Based Digital ID

Security

- Data needs to be secured.
- Only authorized person should access and modify it.

Data Abstraction



- Different level of data should be accessed by different authorized people.

Privacy

- Personal data needs to be private.
- Only authorized person should access it.

Replacement

- In case of identity theft new digital id issuance with modified bio-metrics is needed.

Related Work

Paper	Method	IoT Environment	Remarks
Chen et al.	Entropy Based Key Generation + Reed Solomon ECC + LUT	No	Processing Location Not Specific
Turk et al.	Eigen Function Based FRS + Tracks Head + No Generation of Keys	No	Processing Location Not Specific
Wu et al.	PCA + LUT+ Reed Solomon	No	Processing Location Not Specific
Zhang et al.	Bio Key from Multi Bit Keys	No	Processing Location Not Specific
Oh et al.	Deep Learning Based Method	Yes	Scope Different
Hossain et al.	Bio metric Based + Pairing Based Cryptography	Yes	FR* at Cloud
Masud et al.	Tree Based Cloud Model for Face Recognition	Yes	FA* at Cloud
iFace	**Facial Biometrics + Reed Solomon**	**Yes**	**FA* at Edge**

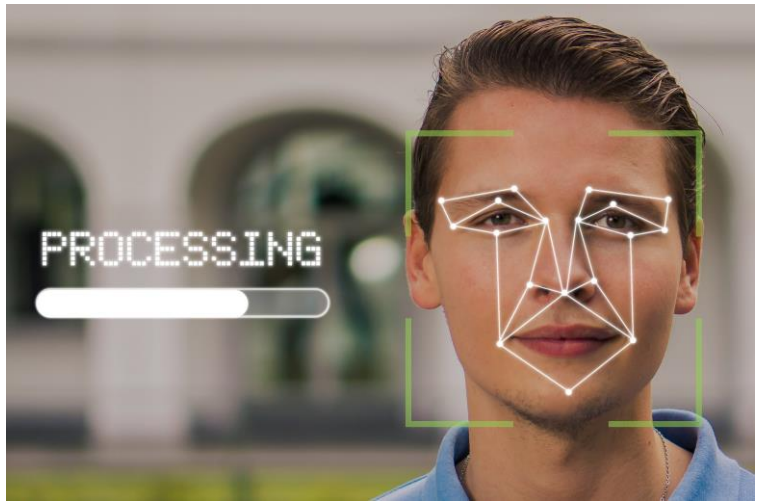
FR* -> Facial Recognition **FA* -> Facial Authentication**

iFace : Digital ID System for Smart City

- Facial Biometric Based

- Two Phases
  - Registration Phase
  - Authentication Phase

- Prerequisite
  - Neutral Frontal Face (NFF) Photo
  - Photo Taken at Edge
  - Photo Taken at Each Time

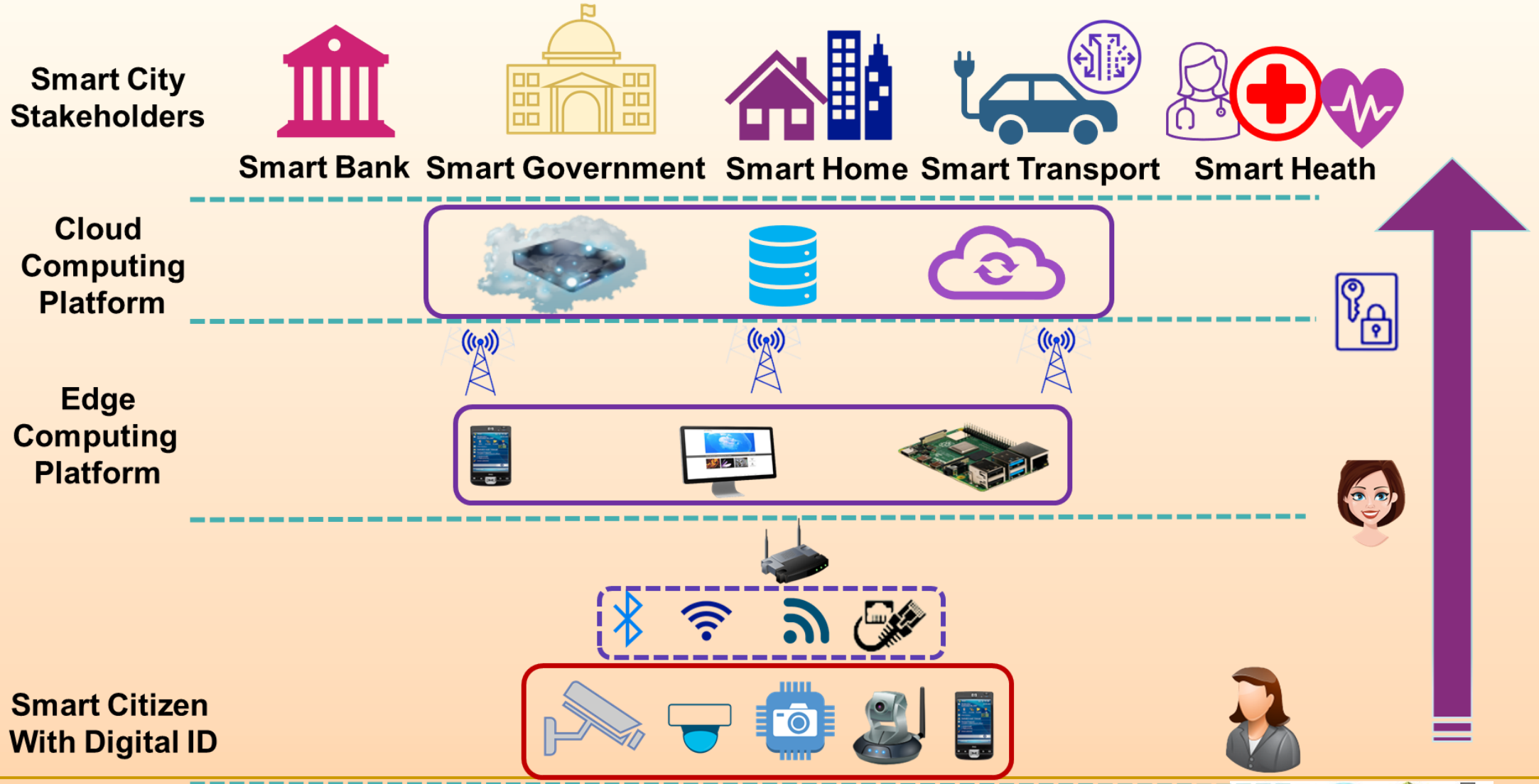


Novel Contribution

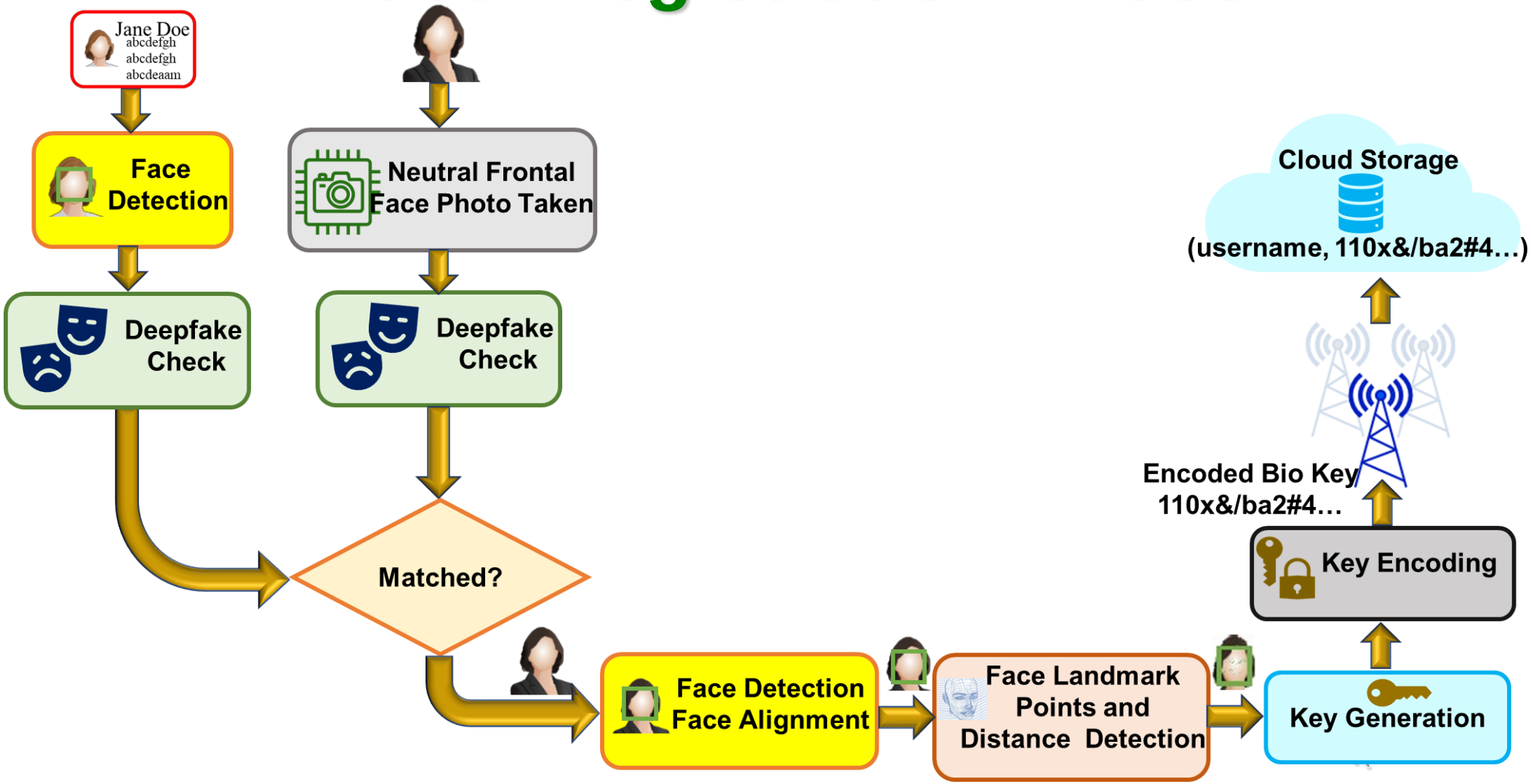
- Registration Process at the Edge.
  - Secured
- Authentication at the Edge too.
  - Free of Indirect Attacks.
- Deepfake Attack Resilient.

- Accommodate Certain Amount of Modified Biometric Data.
- Robust against Unconstrained Environments.
  - Different Lighting Conditions.
  - Light Makeup.

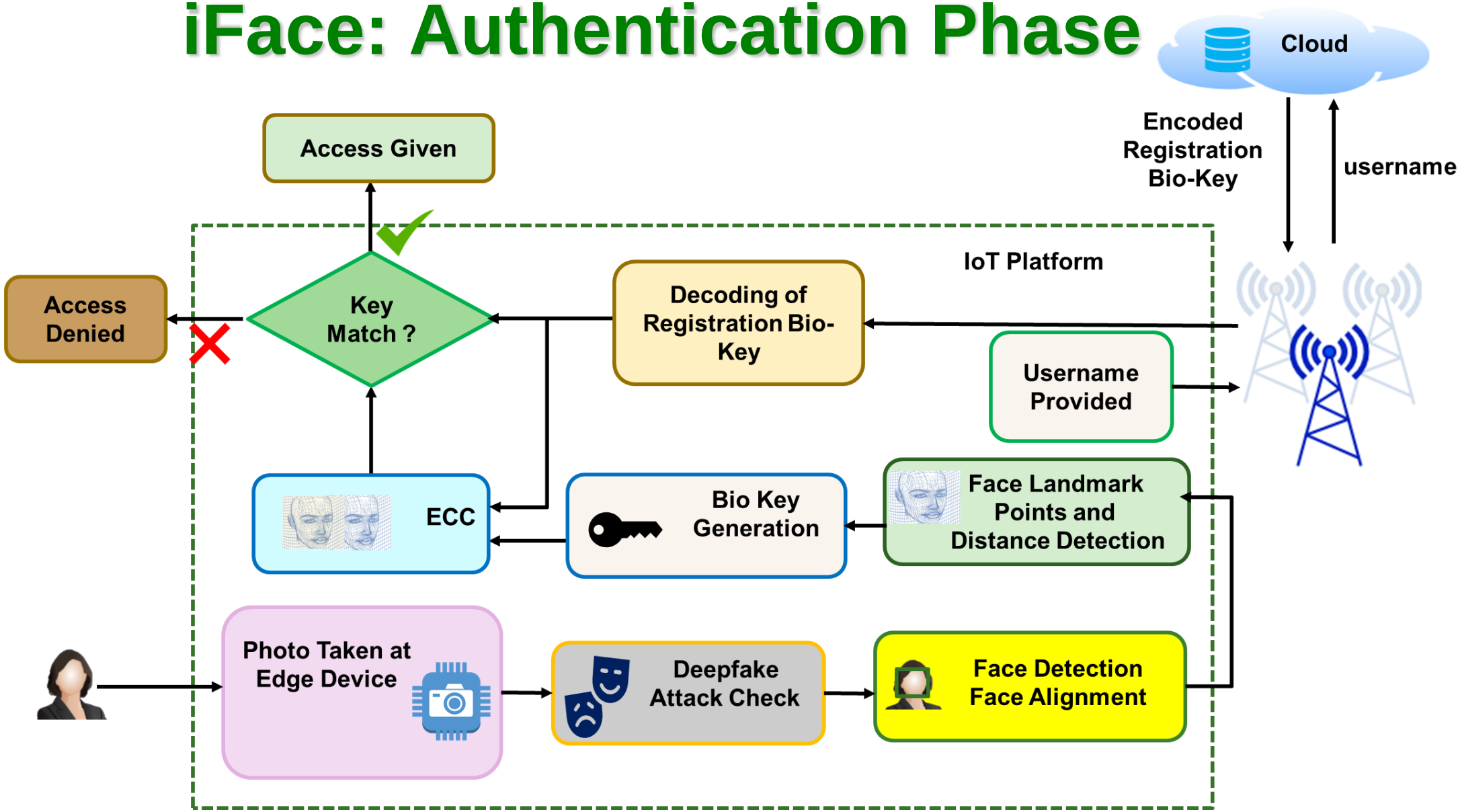
iFace : End-to-End System Level Framework



iFace: Registration Phase



iFace: Authentication Phase



iFace: Implementation

- Implemented in Python.
- Dataset for Deepfake Detection - DeepFakeDetection dataset part of Face Forensics ++.
- For Facial Authentication System 3 Different Datasets.
- Message Length during Error Correction of Encoded Message : 148.
- 4-bit Reed Solomon Codec.

iFace: Dataset Details

Dataset	Source of the Dataset	# of Images
For Deepfake Detection	Part of Face Forensics ++	1,50,000

For iFace Implementation

Dataset Name	Source of the Dataset	# of Images
Dataset -1	CelebA	250
Dataset -2	Frontal Faces Neutral Expression 95 Landmarks	240
Dataset -3	Internet	60

iFace: Sample Images of Dataset

Dataset-1

CelebA

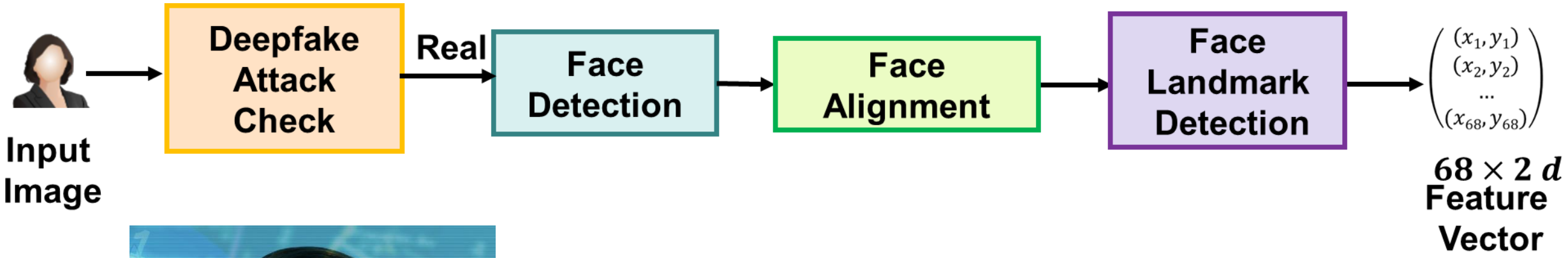
Dataset-2

Frontal Faces Neutral Expression 95 Landmarks

Dataset-3

Internet

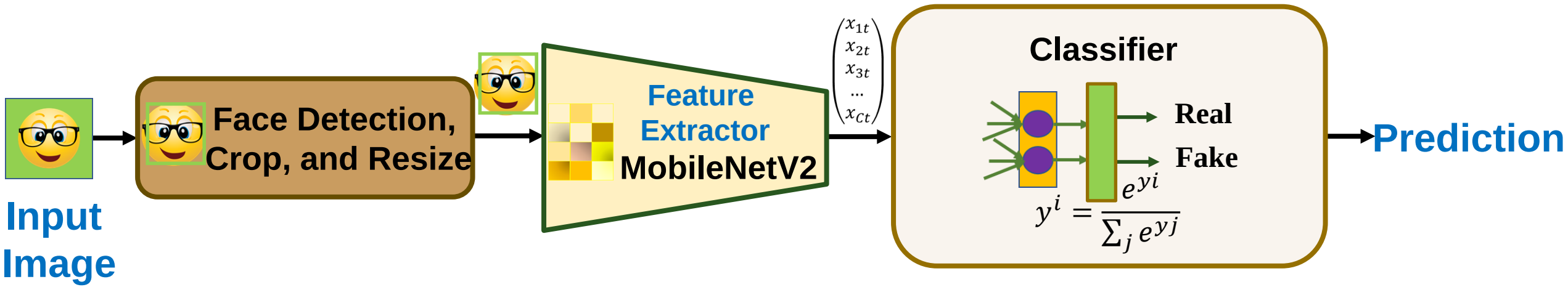
iFace: Face Landmark Points Detection Workflow



- NFF Photo Taken
- Deepfake Detection
- Face Detection & Alignment
- Biometric Features Extraction

iFace : Deepfake Attack Detection

- Feature Extractor : MobileNetV2
- Classifier : Softmax Layer
- Fine tuned a pre-trained MobileNetV2
- Trained last 40 layers in this 53 layers structure



iFace : Face Detection & Alignment

- Face is Detected from NFF photo.
  - dlib library using Histogram of Oriented Gradient (HOG) + Linear Support Vector Machine (SVM).
- Reasons for Choosing HOG Based dlib -
  - Best Choice for Resource Limited HOG based dlib face detector.
  - Fastest and Lightest.
  - Frontal Face Photo No Side View.
  - Model Works Better with CPU. No GPU Required.
- Face Aligned with OpenCV.
  - Limits some positional discrepancies of two photos taken at different times.

iFace : Face Landmark Detection

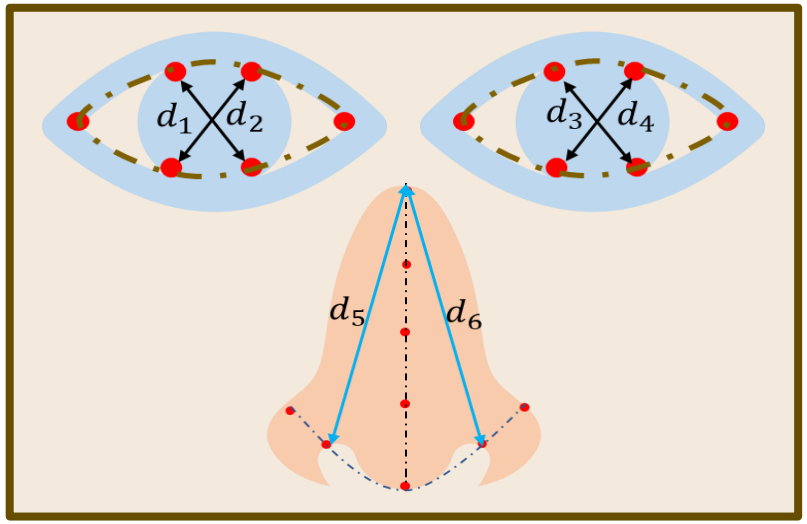
- Detected : 68 facial Landmarks Points related to Jaw, Both Eyebrows and Eyes, Nose, and Mouth.

- Feature Vector *F*1 Size : 68×2

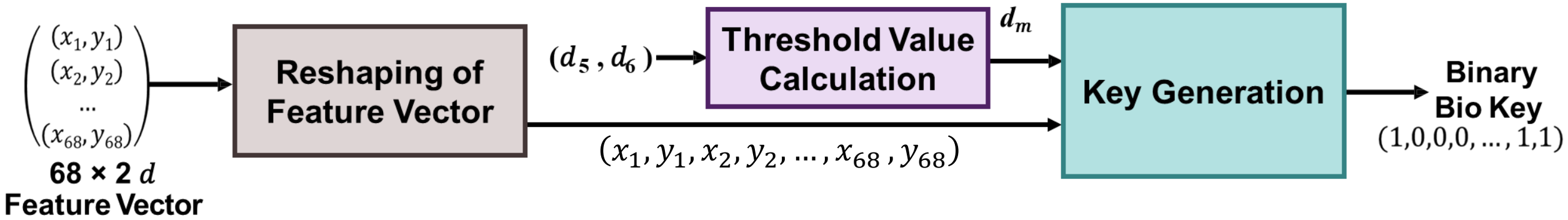
$$\begin{pmatrix} (x_1, y_1) \\ (x_2, y_2) \\ \cdots \\ (x_{68}, y_{68}) \end{pmatrix}$$

- Feature Vector *F*2

$$d_j = d_{1j}$$
$$d_{1j} \in \mathcal{F}2^{(1\times 6)}$$

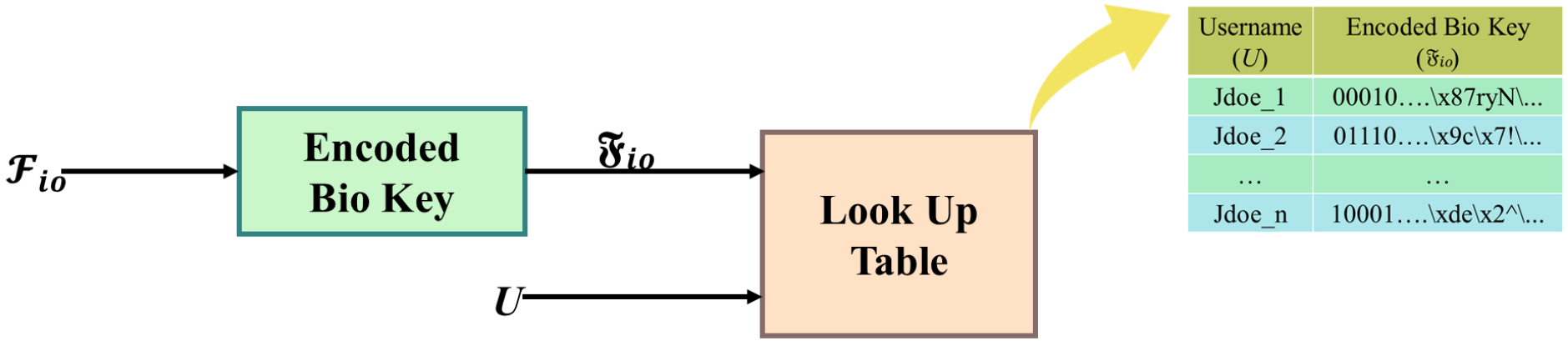


iFace : Biometric Features Extraction



- *F*1 is reshaped : 1 × 136 $(x_1, y_1, x_2, y_2, \dots, x_{68}, y_{68})$
- Threshold Value Calculation $d_m = d_5 + d_6$
- Calculation of $F1_b$ (Binarization of *F1*) $f_{bi} = \begin{cases} 0, & \text{if } f_i < d_m \\ 1, & \text{if } f_i \geq d_m \end{cases}$
- Calculation of Final Feature Vector F_{io} $\boldsymbol{\mathcal{F}}_{io} = \boldsymbol{\mathcal{F}}1_b + \boldsymbol{\mathcal{F}}2$

iFace: New User Registration

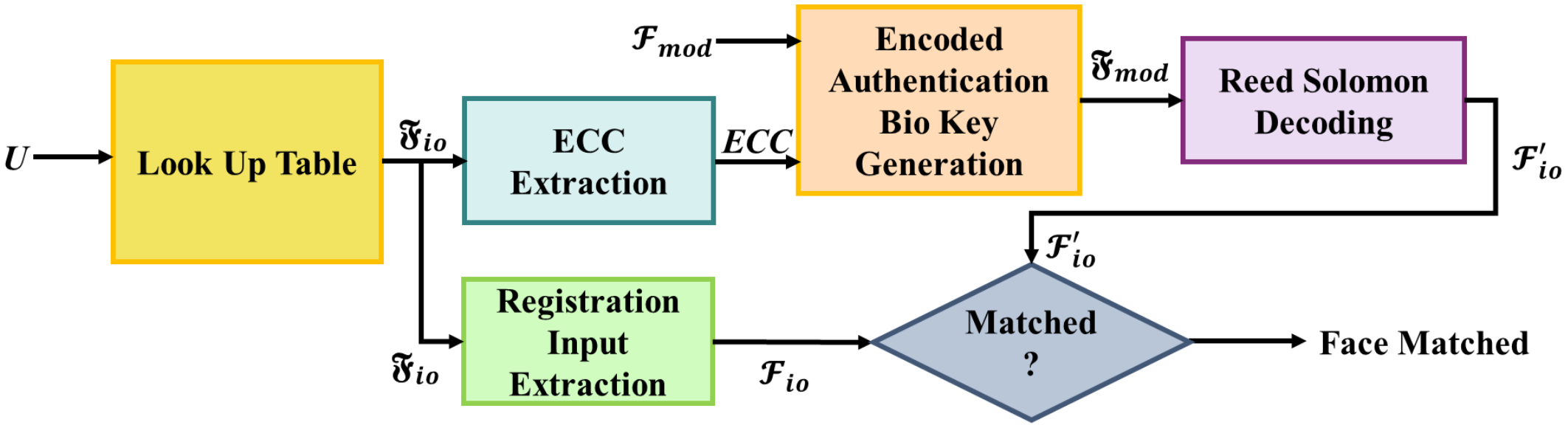


Username (U)	Encoded Bio Key ($\mathfrak{F}_{io}$)
Jdoe_1	00010….\x87ryN\...
Jdoe_2	01110….\x9c\x7!\...
…	…
Jdoe_n	10001….\xde\x2^\...

- Various Times and by Various Cameras of a Smart City Different Photos
- These Variations in Pictures Alter the Bio Key at a Certain Percent
- To Accommodate These Variations and Avoid False Rejection, Reed Solomon (RS) Codes to Correct Errors

iFace: Face Matching Workflow

Authentication Phase



iFace: Metrices

- **FAR :** The percentage of identification instances a Facial Recognition System authorizes an unauthorized person incorrectly.

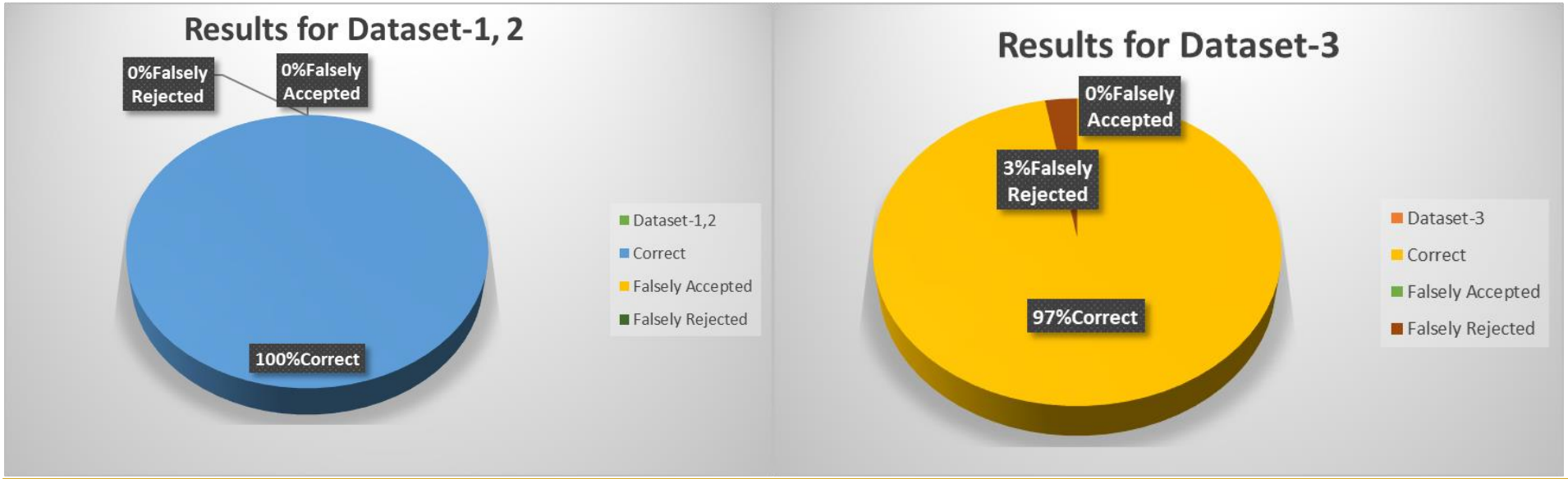
$$FAR = \frac{Number\ of\ False\ Acceptance}{Total\ Number\ of\ Attempts} \times 100\ \%$$

- **FRR :** The percentage of identification instances a Facial Recognition System fails to authorize or identify an authorized person incorrectly.

$$FRR = \frac{Number\ of\ False\ Rejection}{Total\ Number\ of\ Attempts} \times 100\ \%$$

iFace: Performance Evaluation

Dataset	# of Test Image	Correct	Falsely Accepted	Falsely Rejected	Accuracy (%)
Dataset -1	1000	1000	0	0	100 %
Dataset - 2	1000	1000	0	0	100 %
Dataset - 3	900	875	0	25	97.22 %
Total	2900	2875	0	25	99.12 %



FAR = 0%

FRR = 2.77%

iFace: Limitations

- If the person looks considerably different from the photo taken at registration, the system can not authenticate.
- Heavy eye make up like smokey eyes can generate a false rejection.
- Identical twin scenario has not been considered.

iFace & Other Works

Work	IoT Friendly	Scalability	FAR (%)	FRR (%)	Accuracy (%)
iFace	**Yes**	**Any Size of Population for Smart City**	**0**	**2.77**	**99.12**
Hossain et al.	Yes	NA	-	-	97.3 - 99.5
Masud et al.	Yes	NA	-	-	99.4

Conclusions & Future Work

- Biometric based End-to-End Digital ID System of a smart city.
- Our system can detect certain deepfake attacks.
- Does not allow impostors to access users' data.
- Robust to various lighting conditions.
- As a future work,
  - Presentation Attack Detection Module
  - Deepfake Detection Module Update
  - People with glasses, mask, hats and certain age-related changes.
- Scalability Increase.

Thank You!!